

## **REMARKS/ARGUMENTS**

Applicants have received the Office Action dated August 17, 2006, in which the Examiner rejected claims 1-6, 9-12, and 14-56<sup>1</sup> as being based upon a defective reissue declaration. For reasons explained below, Applicants have reinstated the original claim numbering, have amended claims 1, 3-6, 9-12, 14, 16, 18, 20, 22, 34-40, 42-43, 45, 50-52, 55-56, and 58-59, have canceled claims 24, 25, 28, 30, and 32, and have added new claims 62-66. Based on the amendments and arguments contained herein, Applicants believe this case is in condition for allowance.

### **I. STATUS OF THE CLAIMS**

As of the date of this Amendment, claims 1-6, 9-12, 14-25, 28, 30, 32, and 34-61 remain pending<sup>2</sup>. Thus, of the 61 claims presented with the original reissue application, only 53 claims remain pending. With this Amendment, 5 additional claims have been canceled, and five new claims have been added. Further, no new independent claims have been added. Thus, with this Amendment, 53 claims remain pending, and no excess claim fees are due.

### **II. STATUS OF THE SPECIFICATION**

In the Office Action of August 17, 2006, the Examiner did not indicate the status of various amendments to the specification that were still pending prior to the Office Action. In a subsequent telephone interview with Applicant's attorney on December 15, 2006, the Examiner indicated that the remaining outstanding amendments to the specification had been entered. Applicants respectfully request acknowledgement for the record of entry of said specification amendments. The amendments have been included in this paper for reference.

### **III. SPECIAL SUBMISSION REQUIREMENTS**

This Amendment relates to Reissue Application 09/694,416, which is part of a merged proceeding that also includes Reexamination Applications

---

<sup>1</sup> Applicants note that these numbers reflect the claim renumbering introduced by the Preliminary Amendment submitted on April 19, 2006.

<sup>2</sup> To avoid confusion, and in accordance with the rules, all references to the claims in the remainder of this paper follow the original claim numbering as submitted with the original Reissue Application of October 20, 2000, and maintained through the Amendment of June 8, 2005.

90/005,733 and 90/005,776. As a result, this paper is being submitted in triplicate. Further, reexamination 90/005,776 was initiated by a third party. Thus, a Certificate of Service of this Amendment to said third party is included with the submission of this Amendment.

#### **IV. SUPPLEMENTAL REISSUE DECLARATION**

In the Office Action of August 17, 2006, the Examiner rejected the pending claims based upon a defective reissue declaration. The Examiner indicated that a supplemental reissue declaration as required under 37 CFR § 1.175(b)(1) would overcome the rejection. Applicants have included with this Amendment the required declaration, executed by all of the inventors. Applicants respectfully request withdrawal of the rejection.

#### **V. AMENDMENTS TO THE SPECIFICATION**

Applicants have identified additional errors in the specification that were not corrected by previous amendments. Several equations within the paragraph beginning at col. 6, line 24 contain mathematical notation errors. Specifically, the equations defining  $C_1$ ,  $C_2$  and  $C_3$  are written with an equal sign ( $=$ ) instead of a congruence sign ( $\equiv$ ), and the equations defining  $e_1$ ,  $e_2$  and  $e_3$  are written without properly placing parentheses around the modulus portion of the equation. As previously noted by Applicants in the Preliminary Amendment submitted with the Reissue Application, mathematical equations expressing any congruence are written in proper mathematical form as  $b \equiv c \pmod{m}$ , where  $b$  is congruent to  $c$ , and  $m$  is the modulus. The amendments submitted by Applicants correct the above-mentioned equations by expressing the equations in proper mathematical form. Because the new amendments are amendments addressing form, are similar to amendments already entered, and do not add any new matter, Applicants respectfully request that the new amendments be entered.

#### **VI. AMENDMENTS TO THE CLAIMS**

In the Office Action of August 17, 2006, the Examiner did not indicate the status of various claim amendments that were still pending prior to the Office Action. In a subsequent telephone interview with Applicant's agent on October 31, 2006, the Examiner explained that the pending claims would be allowed once

**Appl. Nos. 09/694,416, 90/005,776 & 90/005,733**  
**Amdt. dated February 15, 2007**  
**Reply to Office Action of August 17, 2006**

a properly executed supplemental reissue declaration had been submitted by Applicants. At that time, Applicant's agent indicated to the Examiner that Applicants had identified potential issues with the claim amendments submitted together with Applicant's Request for Continued Examination of April 19, 2006. The claim amendments of April 19, 2006 were in response to the Final Office Action of August 19, 2005, in which the Examiner indicated that dependent claims 32, 33, 37 and 45-49 would be allowable if rewritten in independent form including all the limitations of the base claims and any intervening claims. Applicants Preliminary Amendment of April 19, 2006 incorporated the limitations of dependent claim 33 into each of the independent claims, and canceled claims 26, 27, 29, 31 and 33.

Because of the potential issues raised by the claim amendments of April 19, 2006, Applicants submit herein new amendments to the claims, which incorporate the limitations of dependent claim 32, rather than claim 33, into each of the independent claims. These Amendments are submitted in the present paper in three different formats: in the Listing of Claims presented above, in accordance with the reissue rules; in Appendix A, with changes shown relative to the Amendment of June 8, 2005 (hereinafter, the "Reference Amendment"); and in Appendix B in clean form, without change bars or any other change notation. Applicants again respectfully note that the Examiner had previously indicated that dependent claim 32 would be allowable if rewritten in independent form.

Applicants further note that in the Preliminary Amendment of April 19, 2006, the claims were erroneously renumbered, which created some confusion. To avoid further confusion, and to comply with the reissue rules, the present Amendment presents the claims according to their original numbering as presented in the original Reissue Application, through the Reference Amendment. Because the Office Action of August 19, 2005 was in response to the Reference Amendment, and because the Reference Amendment was the last Amendment to preserve the original claim numbering, the amendments to the claims are described relative to said Reference Amendment for clarity. These relative changes are shown in Appendix A.

**Appl. Nos. 09/694,416, 90/005,776 & 90/005,733**  
**Amdt. dated February 15, 2007**  
**Reply to Office Action of August 17, 2006**

Given the complexity and long history of the present proceedings, and in order to help expedite prosecution of the subject Applications, Applicants submit the following claim-by-claim description of the amendments made to each claim (see also Appendix A for reference):

Claim 1: Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 2: No changes.

Claim 3: One of the subscripts of  $p_{1,2}$  was corrected (1 was changed to i). The recitation of "the class of numbers equivalent to a multiplicative inverse" was amended to recite "a class of numbers equivalent to a multiplicative inverse" to avoid a potential indefiniteness issue. The equation defining ciphertext word signal  $C_x$  was amended to correctly show the subscript y of key portion e and the subscript x of the block message word signal M. Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 4: Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 5: Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The recitation of "the class of numbers equivalent to a multiplicative inverse" was amended to recite "a class of numbers equivalent to a multiplicative inverse" to avoid a potential indefiniteness issue. The word "and" was added in between the recitation of two elements of the second terminal for clarity. The equation defining the ciphertext word signal  $C_B$  was amended to properly show the subscript A of the key

portion e. Similarly, the equation defining the receive message word signal  $M_B'$  was amended to properly show the subscript A of the key portion d. References to  $M_B'$  were amended to read  $M_B'$  for consistency with the other claims and the specification. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 6: Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The equation defining the ciphertext word signal  $C_A$  was amended to properly show the subscript B of the key portion e. Similarly, the equation defining the receive message word  $M_A'$  was amended to properly show the subscript B of the key portion d. References to  $M_A'$  were amended to read  $M_A'$  for consistency with the other claims and the specification.

Claim 7: Canceled.

Claim 8: Canceled.

Claim 9: The preamble was amended to properly refer to "public key signing" for consistency with the body of the claim. The recitation of "the class of numbers equivalent to a multiplicative inverse" was amended to recite "a class of numbers equivalent to a multiplicative inverse" to avoid a potential indefiniteness issue. Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The equation defining the signed message word signal  $M_{1s}$  was amended to properly show the subscript 1 of the key portion d. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 10: A comma was added after the preamble of the claim as a matter of proper form. The signed message word signal was amended from  $M_{As}$  to  $M_{1s}$  for consistency with claim 9, upon which claim 10 depends. The text "to said digital message word signal  $M_1$ " was

added to correct a prior, inadvertent deletion. The equation defining the digital message word signal  $M_1$  was amended to properly show the subscript 1 of the key portion e.

Claim 11: The recitation of "the class of numbers equivalent to a multiplicative inverse" was amended to recite "a class of numbers equivalent to a multiplicative inverse" to avoid a potential indefiniteness issue. The word "digital" was added in front of the recitation of "message word signal  $M_1$ " (in two different places within the claim) for clarity and consistency with the remainder of the claim. The ciphertext word signal  $C_1$  was amended to properly show the number 1 as a subscript. The equation defining the ciphertext word signal  $C_1$  was amended to properly show the subscript 2 of the key portion e. Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 12: The equation defining the message block word signal  $M_1$  was amended to properly show the subscript 2 of the key portion d.

Claim 13: Canceled.

Claim 14: Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 15: No changes.

Claim 16: Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 17: No changes.

Claim 18: The preamble was amended to properly refer to "public key signing" for consistency with the body of the claim. Additional line feeds and

**Appl. Nos. 09/694,416, 90/005,776 & 90/005,733**  
**Amdt. dated February 15, 2007**  
**Reply to Office Action of August 17, 2006**

blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 19: No changes.

Claim 20: The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 21: No changes.

Claim 22: Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 23: No changes.

Claim 24: Canceled.

Claim 25: Canceled.

Claim 26: Canceled.

Claim 27: Canceled.

Claim 28: Canceled.

Claim 29: Canceled.

Claim 30: Canceled.

Claim 31: Canceled.

Claim 32: Canceled.

Claim 33: Canceled.

Claim 34: The claim was amended to recite "the composite number m" instead of "n being equal to a composite number," and further amended to recite "the pair of" prime numbers instead of "2" prime numbers, both amendments incorporated for consistency with claim 14, upon which claim 34 depends. A typographical error was corrected to properly recite "two-prime" RSA public key encryption, rather than "two-rime" RSA public key encryption.

**Appl. Nos. 09/694,416, 90/005,776 & 90/005,733**  
**Amdt. dated February 15, 2007**  
**Reply to Office Action of August 17, 2006**

Claim 35: The claim was amended to recite "RSA public key signing," to recite "the composite number m" instead of "n being equal to a composite number," and to recite "the pair of" prime numbers instead of "2" prime numbers, each amendment incorporated for consistency with claim 9, upon which claim 35 depends.

Claim 36: The claim was amended to recite "the composite number m" instead of "n being equal to a composite number," and further amended to recite "the pair of" prime numbers instead of "2" prime numbers, both amendments incorporated for consistency with claim 16, upon which claim 36 depends.

Claim 37: The claim was amended to recite "the composite number m" instead of "n being equal to a composite number," and further amended to recite "the pair of" prime numbers instead of "2" prime numbers, both amendments incorporated for consistency with claim 18, upon which claim 37 depends.

Claim 38: The claim was amended to recite "the composite number m" instead of "n being equal to a composite number," and further amended to recite "the pair of" prime numbers instead of "2" prime numbers, both amendments incorporated for consistency with claim 20, upon which claim 38 depends.

Claim 39: The claim was amended to recite "the composite number m" instead of "n being equal to a composite number," and further amended to recite "the pair of" prime numbers instead of "2" prime numbers, both amendments incorporated for consistency with claim 22, upon which claim 39 depends.

Claim 40: Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion. A duplicative period at the end of the claim was deleted.

Claim 41: No changes.



**Appl. Nos. 09/694,416, 90/005,776 & 90/005,733**  
**Amdt. dated February 15, 2007**  
**Reply to Office Action of August 17, 2006**

Claim 42: A typographical error was corrected, substituting "and" for "a" where the claim recited "the communications medium sending and receiving messages..." Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 43: Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 44: No changes.

Claim 45: A typographical error was corrected adding the word "to" such that the claim now recites "a data encryption standard (DES) unit coupled to the memory..."

Claim 46: No changes.

Claim 47: No changes.

Claim 48: No changes.

Claim 49: No changes.

Claim 50: The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 51: The relationship defining  $M_i$  was amended to properly recite the relationship as " $M_i \equiv \underline{M}(\text{mod } p_i)$ ."

Claim 52: The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 53: No changes.

Claim 54: No changes.

Claim 55: A spelling error was corrected by amending the word "vai" to properly read "via."

Claim 56: Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of

**Appl. Nos. 09/694,416, 90/005,776 & 90/005,733**  
**Amdt. dated February 15, 2007**  
**Reply to Office Action of August 17, 2006**

dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 57: No changes.

Claim 58: The preamble was amended to properly refer to "public key signing" for consistency with the body of the claim. Additional line feeds and blank lines were added for clarity and consistency with the overall claim format. The limitations of dependent claim 32 were incorporated at the end of the claim, in accordance with the Examiner's suggestion.

Claim 59: The preamble was amended to remove the phrase "the step of," given that the claim is directed to a system, not a method.

Claim 60: No changes.

Claim 61: No changes.

Claim 62: New; a simplified version of canceled claim 26.

Claim 63: New; a simplified version of canceled claim 27.

Claim 64: New; a simplified version of canceled claim 29.

Claim 65: New; a simplified version of canceled claim 31.

Claim 66: New; a simplified version of canceled claim 33.

With regard to the incorporation of the limitations of claim 32 into the independent claims as described above, Applicants note that the limitation refers to a composite number  $m$  as a product of the prime numbers  $p$  and  $q$ . The recitation of the composite number  $m$  underscores an inherent property of the mathematics underpinning the claimed invention as illustrated by the embodiments described within the specification. Specifically, the product of the 3 or more prime numbers  $p_1, p_2, \dots, p_k$  cannot be the same composite number as the product of  $p$  and  $q$ . This is because it is a fundamental theorem of arithmetic that every positive integer can be written uniquely as a product of primes.<sup>3</sup> Thus, because the two composite numbers cannot be the same number (*i.e.*, a single

---

<sup>3</sup> Kenneth H. Rosen, Elementary Number Theory 97 (2<sup>nd</sup> Ed. Addison-Wesley Publishing Company 1988). This reference has been included together with the present Amendment as part of a Supplemental Information Disclosure Statement.

integer cannot be written as two distinct products of primes), the two composite numbers are described within the claim limitation as two distinct composite numbers  $n$  and  $m$ .

Applicants assert that none of the above-described amendments add any new matter. Because the Examiner indicated that dependent claim 32, as presented in the Reference Amendment, was allowable if rewritten in independent form, Applicants respectfully submit that for at least this reason all pending claims as amended, as well as all new claims, are all in condition for allowance.

## **VII. CONCLUSION**


In the course of the foregoing discussions, Applicants may have at times referred to claim limitations in shorthand fashion, or may have focused on a particular claim element. This discussion should not be interpreted to mean that the other limitations can be ignored or dismissed. The claims must be viewed as a whole, and each limitation of the claims must be considered when determining the patentability of the claims. Moreover, it should be understood that there may be other distinctions between the claims and the cited art which have yet to be raised, but which may be raised in the future.

Applicants respectfully request reconsideration and that a timely Notice of Allowance be issued in this case. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fees required (including

**Appl. Nos. 09/694,416, 90/005,776 & 90/005,733**  
**Amdt. dated February 15, 2007**  
**Reply to Office Action of August 17, 2006**

fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "R. de Leon", is written over a horizontal line.

Roberto de Leon  
PTO Reg. No. 58,967  
CONLEY ROSE, P.C.  
(713) 238-8000 (Phone)  
(713) 238-8008 (Fax)  
ATTORNEY FOR APPLICANTS

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
Legal Dept., M/S 35  
P.O. Box 272400  
Fort Collins, CO 80527-2400